Doc Code: AP.PRE.REQ

PTO/SB/33 (01-09)
Approved for use through 02/28/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
D02301

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed name _____

Application Number	Filed
09/576,516	May 23, 2000

First Named Inventor
Xin Qiu

Art Unit	Examiner
2437	PYZOCHA, Michael J.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☑ attorney or agent of record.
Registration number 46201.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Stewart M. Wiener/
Signature

Stewart Wiener
Typed or printed name

215-323-1811
Telephone number

May 18, 2009
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

REQUEST FOR PRE-APPEAL BRIEF REVIEW

Claims 1-19 were rejected under 35 U.S.C. § 103(a) over the combined teachings of U.S. Patent No. 5,870,474 to Wasilewski et al. ("Wasilewski") and U.S. Patent No. 6,324,646 to Chen et al. ("Chen"). For at least the following reasons, this rejection should not be sustained

Claim 1 recites:

> A method of providing varying levels of security in a data processing system, the method comprising:
> receiving information from an outside source;
> *retrieving a first indicator from the received information that instructs the system to operate at a higher level of security*;
> receiving further information from said outside source;
> retrieving a separate second indicator from said further information received from said outside source, *the second indicator for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator*;
> *receiving an encrypted message that authorizes the system to operate at the lower level of security*;
> authenticating the encrypted message; and
> *preventing operation at the lower level of security until a decrease in security levels is indicated by said second indicator and the encrypted message*; while
> *continuing operation of said processing system at the higher level of security.*

(Emphasis added).

In contrast, Wasilewski does not teach or suggest the subject matter of claim 1. Rather, Wasilewski teaches a control system for conditional access to a media program in which "program bearing packets are encrypted according to a first encryption algorithm using a first key, which is then encrypted according to a second encryption algorithm using a second key. The first keys are transported in packets to the customer's set top units along with the program packets. A public key cryptographic technique encrypts the second key such that the public key used in the encryption corresponds to the private key of the customer's set top unit. After the conditional access layers have been added, the packets are encapsulated and output in a second network protocol destined for the set top unit." (Wasilewski, abstract).

In particular, Wasilewski completely fails to teach or suggest a system configured to operate at a higher (or lower) level of security in response to receiving an "indicator…that instructs the system to operate at a higher [or lower] level of security." (claim 1). Rather, Wasilewski merely teaches a system in which media content experiences multiple levels of

encryption with different corresponding encryption keys prior to delivery to a set top box. (*See e.g.* Wasilewski, abstract and col. 11, lines 10-23). To maintain security, Wasilewski teaches that "frequent key changing is designed to thwart attempts by unauthorized users to compromise the encryption algorithm by discovering the key." (Wasilewski, col. 8, lines 48-52).

The recent Office Action improperly extrapolates from these teachings that Wasilewski's system is necessarily operating at a different level of security whenever an encryption/decryption key is changed, thereby allegedly rendering obvious much of the subject matter of claim 1. (Action, pp. 3-4). However, this assertion is completely without basis and incongruous with the principles taught by Wasilewski. It will be readily apparent to anyone having ordinary skill in the art that the level of security at which data is transmitted and received is determined by the algorithm(s) used to encrypt the data, and not by the specific parameters (i.e. encryption keys) used by the algorithms to obtain unique encryption results. In other words, changing an encryption key in an encrypted system from a first value to a second value does not make the encrypted data any more or less inherently secure in its encryption. Instead, the security of the encryption is determined by the encryption algorithm itself, not by the parameters passed to the algorithm. Thus, without a change in the encryption algorithm itself, no measurable change in the security level of an encrypted system is feasible. Wasilewski does not teach or suggest any such change in any of the nested algorithms used to encrypt media content data. Thus, even though Wasilewski teaches that the keys used to encrypt data may be changed, Wasilewski does not teach or suggest a change in the actual level of security in data transmission. Wasilewski merely teaches *static* encryption algorithms with *dynamic* parameters.

In response, the final Office Action asserts that "one of ordinary skill recognizes that keys have different strengths and therefore different levels of security." (Action, p. 7). Applicant strongly disagrees. In making this assertion the Examiner is essentially arguing that two different keys used with the same exact algorithm could inherently result in different levels of encryption. Such an argument is contrary to the basic principles of encryption. Applicant rejects the notion that one of ordinary skill in the art would subscribe to the idea that different keys used with the same algorithm would result in different levels of security. Applicant further notes that the final Office Action has failed to provide any evidence in support of this position.

The mere assertion by the Examiner that something is well-known in the art does not make it so.

Without teaching a change in the level of security, Wasilewski *cannot* teach much of the subject matter of claim 1. Specifically, Wasilewski *cannot* teach the steps of "receiving a first indicator from the received information that instructs the system to operate at a higher level of security," "retrieving a separate second indicator…for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator," receiving and authenticating "an encrypted message that authorizes the system to operate at the lower level of security," and "preventing an operation at the lower level of security until a decrease in security levels is indicated by said second indicator and the encrypted message." (claim 1).

Turning now to Chen, it becomes readily apparent that Chen also does not teach or suggest much of the subject matter of claim 1. Chen teaches a data transmission protocol having a "security descriptor field identifier, whose implementation can be understood by communicating parties." (Chen, col. 6, lines 28-31). However, Chen does not teach or suggest that the security descriptor field identifier may be *dynamically changed by the communicating parties during the transmission of data* to alter the level of security in response to retrieving an "indicator from the received information that instructs the system to operate at a higher [or lower] level of security." (claim 1). Rather, Chen appears to merely teach that the data protocol used between communicating parties provides for flexibility in upgrading algorithms used to secure data transmitted between those parties.

Moreover, Chen does not teach or suggest anywhere that both an "indicator for instructing the system to operate at a lower level of security than the higher level of security" and "an encrypted message that authorizes the system to operate at a lower level of security" must be received in addition to the encrypted message being authenticated prior to a system switching from a higher level of security to a lower level of security. (claim 1). Chen simply does not teach or suggest this change in the level of security or the requirements that must be met to effect it.

Under the analysis required by *Graham v. John Deere*, 383 U.S. 1 (1966) to support a rejection under § 103, the scope and content of the prior art must first be determined, followed

by an assessment of the differences between the prior art and the claim at issue in view of the ordinary skill in the art. In the present case, the scope and content of the prior art, as evidenced by Wasilewski and Chen, did not include the claimed subject matter, particularly the following steps:

- "retrieving a first indicator from the received information that instructs the system to operate at a higher level of security;"
- "retrieving a separate second indicator from said further information…for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator;"
- "receiving an encrypted message that authorizes the system to operate at the lower level of security;"
- "authenticating the encrypted message;" and
- "preventing operation at the lower level of security until a decrease in security levels is indicated by said indicator and the encrypted message; while continuing operation of said processing system at the higher level of security."

(claim 1).

The differences between the cited prior art and the claimed subject matter are significant because the claimed method provides a way to "make a change from a low level of encryption to a high level of encryption in a relatively easy manner" without "[compromising a system] when a change is made from a high level of security to a low level of security." (Applicant's specification, p. 2, lines 4-7). Thus, the claimed subject matter provides features and advantages not known or available in the cited prior art. Consequently, the cited prior art will not support a rejection of claim 1 under 35 U.S.C. § 103 and *Graham*. For at least these reasons, the rejection of claim 1 and its corresponding dependent claims based on Wasilewski and Chen should be reconsidered and withdrawn.

Additionally, various dependent claims of the application recite subject matter that is further patentable over the cited prior art. Specific, non-exclusive examples follow.

Claim 2 recites "wherein the encrypted message comprises a Decreased-Security-Authorization-Code." Claims 3-5 impose additional limitations on the Decreased-Security-

Authorization-Code. As has been amply demonstrated above, neither of Wasilewski and Chen teaches or suggests even the existence of an "encrypted message that authorizes the system to operate a lower level of security," let alone the additional limitations imposed on the encrypted message by dependent claims 2-5. The Office Action again attempts to assert that a change in an encryption key indicates a change in a level of security, an assertion that, as has been amply demonstrated above, is plainly incorrect. (Action, pp. 3-4).

The final Office Action further asserts that "the encrypted messages of Wasilewski including the indicator of Chen to lower the security correspond to the Decreased-Security-Authorization-Code which can lower the encryption and/or authentication." (Action, pp. 7-8). Applicant respectfully disagrees, noting that as taught in claims 2-5 and Applicant's specification, a Decreased-Security-Authorization-Code is more than a simple instruction to change an encryption key. (*See* Applicant's specification, p. 6). Rather, the Decreased-Security-Authorization-Code is an explicit indication and authorization to its receiver that the security level will be decreased. The final Office Action has failed to demonstrate that the receiver of Wasilewski interprets any message as authorizing a decrease in security. Rather, the final Office Action appears to argue that when the receiver of Wasilewski by receives a change in an encryption key, the receiver is not only cognizant that the encryption key represents a reduced level of security, but that the encryption key itself is an explicit authorization of a reduced level of security. Wasilewski simply does not teach or suggest this subject matter. For at least these additional reasons, the rejection of claims 2-5 should be reconsidered and withdrawn.

Claim 14 recites "using a Key Management Message to convey said Decreased Security Authorization Code." Claims 15-17 recite further limitations on the Key Management Message. Again, with respect to these claims, the recent Office Action cites to the same portion of Wasilewski used elsewhere. (Action, p. 4) (*citing to* Wasilewski, col. 11 lines 10-50). Aside from the utter irrelevance of the cited portion, as neither of Wasilewski and Chen teaches or suggests a Decreased Security Authorization Code at all, Wasilewski and Chen combined *cannot* teach or suggest "using a Key Management Message to convey said Decreased Security Authorization Code." For at least this additional reason, the rejection of claims 14-17 should be reconsidered and withdrawn.